ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 212.268.03 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР) МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 23 марта 2017 г. № 2

О присуждении Терновому Олегу Степановичу, гражданину Российской Федерации, учёной степени кандидата технических наук.

Диссертация «Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности при DDoS-атаках» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 28 декабря 2016 г. (протокол № 24) диссертационным советом Д 212.268.03 на базе ТУСУРа (634050, г. Томск, пр. Ленина, 40). Приказ о создании диссертационного совета № 105/нк от 11.04.2012 г.

Соискатель Терновой Олег Степанович, 1983 года рождения, в 2006 г. окончил федеральное государственно бюджетное образовательное учреждение высшего образования «Алтайский государственный университет» (АлтГУ). С 2011 по 2015 г. обучался в аспирантуре АлтГУ. Работает начальником отдела информационных технологий и инноваций в образовании АлтГУ, старшим преподавателем кафедры информатики факультета математики и информационных технологий АлтГУ.

Диссертация выполнена на кафедре вычислительной техники и электроники физико-технического факультета АлтГУ.

Научный руководитель – Шатохин Александр Семенович, кандидат технических наук, доцент, директор центра электронных образовательных ресурсов, доцент кафедры информатики, вычислительной техники и информационной безопасности федерального государственного образовательного учреждения высшего образования «Алтайский государственный технический университет им. И.И. Ползунова».

Официальные оппоненты: Захаров Александр Анатольевич, доктор технических наук, профессор, заведующий кафедрой информационной безопасности федерального государственного автономного образовательного учреждения высшего образования «Тюменский государственный университет»; Рева Иван Леонидович, кандидат технических наук, доцент, доцент кафедры защиты информации, декан факультета автоматики и вычислительной техники федерального государственного бюджетного образовательного учреждения высшего образования «Новосибирский государственный технический университет», дали положительные отзывы на диссертацию.

Ведущая организация — федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технологический университет» (МИРЭА), в своем положительном заключении, подписанном Лосем В.П., д.в.н., профессором, советником ректора, заведующим кафедрой «Управление и моделирование систем» МИРЭА и утвержденном Соколовым В.В., д.ф.-м.н., профессором, первым проректором МИРЭА, указала, что диссертация является законченной научно-квалификационной работой, в которой содержится решение научной задачи, имеющей важное хозяйственное значение, разработан ряд научных положений, совокупность которых можно квалифицировать как вклад в выбранное научное направление. Диссертация имеет научную и практическую значимость. Заключение рассмотрено на научном семинаре кафедры КБ-3 «Управление и моделирование систем» МИРЭА (протокол № 6 от «30» января 2017 г.).

Соискатель имеет 17 опубликованных работ, в том числе по теме диссертации 10 работ, включая 5 работ из перечня ВАК и 2 свидетельства о регистрации программы для ЭВМ. Общий объем опубликованных работ — 5,3 п.л., авторский вклад по теме диссертации — 1,85 п.л. Наиболее значимые работы:

1. Терновой О.С. Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности в результате DDoS-атак // Известия Алтайского государственного университета. – 2013. №1/2(77). – С. 123–126.

2. Терновой О.С. Снижение ошибки обнаружения DDoS-атак статистическими методами при учете сезонности / О.С. Терновой, А.С. Шатохин // Ползуновский вестник. – 2012. – №3/2. – С. 226 – 229.

3. Терновой О.С. Использование байесовского классификатора для получения обучающих выборок, позволяющих определять вредоносный трафик на коротких интервалах / О.С. Терновой, А.С. Шатохин // Известия Алтайского государственного университета. – 2013. №1/1(77). – С. 151–153.

4. Терновой О.С. Ранее обнаружение DDoS-атак статистическими методами при учете сезонности / О.С. Терновой, А.С. Шатохин // Доклады Томского государственного университета. – 2012. – №1/2 (25) – С.104–108.

5. Терновой О.С. Методики и средства выявления и противодействия угрозам информационной безопасности в контексте региональных web-ресурсов / О.С. Терновой, А.С. Шатохин // Региональные аспекты технической и правовой защиты информации: монография. – Барнаул: Изд-во АлтГУ, 2013. – С.106 –123.

На диссертацию и автореферат поступило 4 положительных отзыва из следующих организаций: Омский государственный технический университет (Щерба Е.В., кандидат технических наук, доцент, доцент кафедры комплексной защиты информации); Новосибирский государственный университет экономики и управления (Пестунова Т.М., кандидат технических наук, доцент, заведующий кафедрой информационной безопасности); Югорский государственный университет, г.Ханты-Мансийск (Семенов С.П., кандидат физ.-мат. наук, профессор кафедры систем обработки информации, моделирования и управления); Самарский национальный исследовательский университет им. Академика С.П. Королева, (Осипов М.Н., кандидат физ.-мат. наук, доцент, заведующий кафедрой безопасности информационных систем).

В отзывах на диссертацию и автореферат указаны следующие основные замечания: в тексте работы везде упоминается конкретный класс DOS атак – HTTP Flood, однако в теме исследования заявлены методы защиты от DDOS атак в общем смысле; выбор метода кластеризации K-means не выглядит достаточно убедительно; в работе отсутствует наглядное представление экспериментальных

данных или ссылки на работы, объясняющие то, откуда эти данные взяты; второй, выносимый на защиту результат, является давно известным фактом, как таковая сезонность проявляется в явном виде на федеральных либо региональных онлайн-сервисах; отсутствует описание ограничения использования разработанного программного средства; недостаточно проработаны модели DDoS–атака, обнаружение которых рассматривается в работе.

Выбор официальных оппонентов обосновывается тем, что д.т.н. проф. Захаров А.А. является известным ученым в области обеспечения защиты телекоммуникационных сетей; к.т.н. доцент Рева И.Л. является известным специалистом по проектированию и разработке специального программного обеспечения в области информационной безопасности. Выбор ведущей организации (МИРЭА) обосновывается тем, что она имеет общепризнанные достижения в области информационной безопасности и защиты информации, институт комплексной безопасности и специального приборостроения и высококвалифицированных специалистов в области разработки методов, алгоритмов, программных средств в решении задач информационной безопасности, способных определить и аргументировано оценить научную и практическую значимость диссертационной работы Тернового О.С.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– **разработаны** новая методика и средство раннего выявления и противодействия угрозам нарушения информационной безопасности при DDoS–атаках, позволяющие учитывать сезонность в сетевой нагрузке и выполнять обнаружение вредоносных запросов на ранней стадии DDoS–атак;

– **предложены** новый алгоритм обнаружения и блокирования вредоносных запросов, формальное описание «сезонности» сетевого трафика, позволяющие увеличить защищенность конечных сетевых ресурсов;

– **доказана** эффективность применения полученных научных результатов для обеспечения безопасности сетевых ресурсов при распределенных атаках, направленных на отказ в обслуживании.

Теоретическая значимость работы обосновывается тем, что:

– **изложена** методика раннего обнаружения и противодействия распределенным атакам, направленным на отказ в обслуживании. Особенностями методики являются: учет «сезонных» периодов, ориентация использования на конечном ресурсе, универсальность;

– **изучены** факторы, влияющие на формирование «сезонности» сетевого ресурса;

– **проведена модернизация** модели обнаружения начала распределенных атак, направленных на отказ в обслуживании, особенностью модели является учет «сезонности» в работе сетевого ресурса, который был применен впервые.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– **разработано и внедрено** в деятельность предприятий и учебный процесс вузов методическое и программно-алгоритмическое обеспечение;

– **созданы** методика и программное обеспечение по выявлению и противодействию угрозам нарушения информационной безопасности при DDoS-атаках;

– **представлены** предложения по дальнейшему усовершенствованию механизмов защиты сетевых ресурсов.

Оценка достоверности результатов исследования выявила: непротиворечивость результатов, полученных как на промежуточных, так и на окончательных этапах работы; согласованность с результатами проведенных практических экспериментов в сравнении с другими подходами и аналогами. Совет отмечает достаточный уровень опубликованности основных результатов диссертации в профильных журналах.

Личный вклад состоит в непосредственном участии соискателя в научных экспериментах и получении исходных данных, исследовании сезонности сетевого трафика, разработке методического, алгоритмического и программного обеспечения для решения поставленных задач, обработке и интерпретации экспериментальных данных.

Диссертация Тернового О.С. на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, ин-

формационная безопасность» является научно-квалификационной работой, в которой содержится решение важной задачи раннего обнаружения вторжений, имеющей существенное значение для обеспечения безопасности вычислительных сетей, что соответствует требованиям п. 9 «Положения о порядке присуждения ученых степеней».

На заседании 23 марта 2017 г. диссертационный совет принял решение присудить Терновому О.С. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 9 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за — 18, против — 1, недействительных бюллетеней — 0.

Зам. председателя
диссертационного совета Шурыгин Юрий Алексеевич

Ученый секретарь
диссертационного совета Зыков Дмитрий Дмитриевич

«24» марта 2017 г.